UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity) *(Only for new nonprovisional applications under 37 CFR 1.53(b))*	Docket No. EN998146
	Total Pages in this Submission 3

TO THE ASSISTANT COMMISSIONER FOR PATENTS
Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA

jc675 U.S. PTO 09/443204 11/18/99

and invented by:

John Edward Fetkovich, Wai Man Lam, and George William Wilhelm, Jr.

If a **CONTINUATION APPLICATION**, *check appropriate box and supply the requisite information:*

☐ **Continuation**   ☐ **Divisional**   ☐ **Continuation-in-part (CIP)**   of prior application No.: _____

Which is a:

☐ **Continuation**   ☐ **Divisional**   ☐ **Continuation-in-part (CIP)**   of prior application No.: _____

Which is a:

☐ **Continuation**   ☐ **Divisional**   ☐ **Continuation-in-part (CIP)**   of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below

2. ☒ Specification having _____ 33 _____ pages and including the following:

    a. ☒ Descriptive Title of the Invention

    b. ☒ Cross References to Related Applications *(if applicable)*

    c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*

    d. ☐ Reference to Microfiche Appendix *(if applicable)*

    e. ☒ Background of the Invention

    f. ☒ Brief Summary of the Invention

    g. ☒ Brief Description of the Drawings *(if drawings filed)*

    h. ☒ Detailed Description

    i. ☒ Claim(s) as Classified Below

    j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL **(Large Entity)** *(Only for new nonprovisional applications under 37 CFR 1.53(b))*	Docket No. EN998146
	Total Pages in this Submission 3

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*

    a. ☒ Formal   Number of Sheets   **Two (2)**

    b. ☐ Informal   Number of Sheets

4. ☒ Oath or Declaration

    a. ☒ Newly executed *(original or copy)*   ☐ Unexecuted

    b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*

    c. ☒ With Power of Attorney   ☐ Without Power of Attorney

    d. ☐ *DELETION OF INVENTOR(S)*
        Signed statement attached deleting inventor(s) named in the prior application,
        see 37 C.F.R. 1.63(d)(2) and 1.33(b).

5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
     The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ☐ Computer Program in Microfiche *(Appendix)*

7. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*

    a. ☐ Paper Copy

    b. ☐ Computer Readable Copy *(identical to computer copy)*

    c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☒ Assignment Papers *(cover sheet & document(s))*

9. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*

10. ☐ English Translation Document *(if applicable)*

11. ☒ Information Disclosure Statement/PTO-1449   ☒ Copies of IDS Citations

12. ☐ Preliminary Amendment

13. ☒ Acknowledgment postcard

14. ☒ Certificate of Mailing

     ☐ First Class   ☒ Express Mail *(Specify Label No.):*   EL172581550US

UTILITY PATENT APPLICATION TRANSMITTAL **(Large Entity)** *(Only for new nonprovisional applications under 37 CFR 1.53(b))*	Docket No. **EN998146**	
	Total Pages in this Submission **3**	

Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. ☐ Additional Enclosures *(please identify below):*

Fee Calculation and Transmittal

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate		Fee
Total Claims	38	- 20 =	18	x	$18.00	$324.00
Indep. Claims	4	- 3 =	1	x	$78.00	$78.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
					BASIC FEE	$760.00
OTHER FEE *(specify purpose)* _____						$0.00
					TOTAL FILING FEE	$1,162.00

☐ A check in the amount of _____ to cover the filing fee is enclosed.

☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. 09-0457 (IBM) as described below. A duplicate copy of this sheet is enclosed.

    ☒ Charge the amount of **$1,162.00** as filing fee.

    ☒ Credit any overpayment.

    ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.

    ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

William H. Steinberg
                   Signature
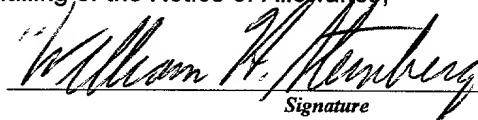
Dated: _____

    William H. Steinberg, Esq.
    Reg. No. 28,540
    IBM Corporation
    Intellectual Property Law
    1701 North Street
    Endicott, N.Y. 13760
    Tel.: (607) 755-0123
    Fax: (607) 755-3250

CC:

     P01ULRG/REV04

CERTIFICATE OF MAILING BY "EXPRESS MAIL"

In Re Application of: Fetkovich et al.

Title: DYNAMIC ENCRYPTION AND DECRYPTION OF A
STREAM OF DATA

Attorney Docket No.: EN998146

"EXPRESS MAIL" MAILING LABEL NO.   EL172581550US

Date of Deposit   11/18/99

I hereby certify that this paper is being deposited
with the U.S. Postal Service "Express Mail Post Office
to Addressee" service under 37 CFR 1.10 on the date
indicated above, and addressed to Assistant
Commissioner for Patents, Box PATENT APPLICATION,
Washington, D.C. 20231

Enclosed: New Utility Patent Application Transmittal
Letter (Large Entity) (3 pages, in
duplicate)
U.S. Patent Application -
Specification (20 pages); Claims (12 pages);
Abstract (1 page)
Formal Drawings (2 sheets)
Declaration and Power of Attorney (4 pages)
(___unsigned) (xx signed)
Assignment w/Recordation Cover Sheet
(2 pages)
Information Disclosure Statement (1 page)
Information Disclosure Citation w/references
(1 page) (5 cited)
2 Postcards

Denise M. Jurik

(Typed or printed name of person mailing paper or fee)
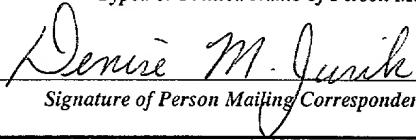
(Signature of person mailing paper or fee)

APPLICATION

FOR

UNITED STATES LETTERS PATENT

APPLICANT(S) NAME: J. E. Fetkovich et al

TITLE: DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA

DOCKET NO.   EN998146

INTERNATIONAL BUSINESS MACHINES CORPORATION

DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA

Cross-Reference to Related Application

This application is related to commonly assigned, co-pending patent application serial number 08/881,139, filed

5 June 24, 1997 by Ciacelli et al. and entitled "Apparatus, Method And Computer Program Product For Protecting Copyright Data Within A Computer System," which is hereby incorporated herein by reference in its entirety.

10 ## Technical Field

The present invention is directed in general to protection of digital data and, more particularly, to techniques for dynamically encrypting and decrypting compressed digital video or audio for secure digital

15 transmission of the data.

Background of the Invention

The advent of world-wide electronic communications

20 systems has enhanced the way in which people can send and receive information. For example, the capabilities of real-time video and audio systems have greatly improved in recent years. In order to provide services such as video-on-demand, video conferencing, and motion picture playback, to

25 name but a few, an enormous amount of bandwidth is required. In fact, bandwidth is often the main inhibitor in the effectiveness of such systems.

In order to overcome the constraints imposed by existing technology, compression systems have emerged.

These systems reduce the amount of video and audio data which must be transmitted by removing redundancy in the picture sequence. At the receiving end, the picture sequence is uncompressed and may be displayed in real time.

5   One example of a video compression standard is the Moving Picture Expert's Group (MPEG) standard. Within the MPEG standard (known as ISO/IEC 13818), video compression is defined within a picture and between pictures. Video compression within a picture is accomplished by conversion
10   of the digital image from the time domain to the frequency domain by a discrete cosine transform, quantitization, variable length coding, and Huffman coding. Compression between pictures is accomplished by a process referred as "motion estimation", in which a motion vector plus
15   difference data is used to describe the translation of a set of picture elements from one picture to another. The ISO MPEG2 standard specifies only the syntax of a bit stream and semantics of the decode process. The particular choice of coding parameters and trade-offs in performance
20   versus complexity are left to the system developers.

There is substantial interest in the computer and entertainment industries in incorporating video data in multimedia and related applications for use on processor-based video systems. Potential growth in this area has
25   been enabled by development of video compression schemes, such as the above-summarized MPEG standard that reduce the amount of digital data required to display high quality video images, and by the development of storage media, such

as digital video discs (DVDs) which can accommodate data in compressed form for an entire movie on a single compact disc. With the compressed data of an entire movie readily available on a single compact disc, content providers are

5   naturally concerned with the possibility of unauthorized copying, and thus, desire to encrypt the compressed data wherever it may be available.

As digital transmissions (and storage) become more prevalent, the security of these transmissions becomes more

10   important. The owners and distributors of any digital signal, such as a video conferencing signal or a direct-satellite transmission, may wish the signal to be unintelligible to unauthorized parties. A digital transmission of video (such as MPEG compressed data) can be

15   protected by encrypting the data. Various encryption techniques exist in the literature for protecting a data stream. Decryption of the stream is then performed on the receiving end. Encryption and decryption might depend on a numerical key. Such a scheme, depending on the

20   thoroughness of the encryption, may be secure for a time, but the stream is still susceptible to being intercepted and reverse engineered.

Thus, a more secure approach to encrypting a digital transmission, either within a system or between systems is

25   deemed desirable.

Disclosure of the Invention

To briefly summarize, provided herein in one aspect is a method for protecting a stream of data to be transferred between an encryption unit and a decryption unit. The method includes: encrypting the stream of data at the encryption unit for transfer thereof from the encryption unit to the decryption unit; dynamically varying the encrypting of the stream of data at the encryption unit by changing at least one encryption parameter and signaling the change in encryption parameter to the decryption unit, wherein the dynamically varying is responsive to occurrence of a predefined condition in the stream of data; and decrypting the encrypted data at the decryption unit, the decrypting accounting for the dynamic varying of the encrypting by the encryption unit using the changed encryption parameter. In an enhanced embodiment, changing of the encryption parameter to accomplish the dynamically varying includes changing at least one of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger.

In another aspect, a system for protecting a stream of data is provided which includes an encryption unit for encrypting the stream of data for transfer to a decryption unit, as well as means for dynamically varying the encrypting of the stream of data by the encryption unit by changing at least one encryption parameter and signaling

the change to the decryption unit. The means for
dynamically varying the encrypting of the stream is
responsive to occurrence of a predefined condition in the
stream of data. The decryption unit is adapted to decrypt
5   the encrypted data accounting for the dynamic varying of
the encrypting by the encryption unit using the changed
encryption parameter.

In a further aspect, provided herein is at least one
program storage device readable by a machine, tangibly
10   embodying at least one program of instructions executable
by the machine to perform a method for protecting a stream
of data to be transferred between an encryption unit and a
decryption unit. The method includes: encrypting the
stream of data at the encryption unit for transfer thereof
15   to the decryption unit; dynamically varying the encrypting
of the stream of data at the encryption unit by changing an
encryption parameter and signaling the change in encryption
parameter to the decryption unit, wherein the dynamically
varying is responsive to occurrence of a predefined
20   condition in the stream of data; and decrypting the
encrypted data at the decryption unit, the decrypting
accounting for the dynamic varying of the encrypting by the
encryption unit using the changed encryption parameter.

To restate, provided herein is a technique for more
25   securely encrypting a stream of digital data for
transmission using a relatively small, yet flexible set of
encryption parameters. The set of encryption parameters is
employed to dynamically vary the encryption of the stream

of data, such as a stream of MPEG compressed data. The set
of encryption parameters may comprise one or more of an
encryption key, an encryption granularity, an encryption
density scale, an encryption density, an encryption delay,
an encryption key update variable, and an encryption key
update data trigger. The encryption parameter set employed
is easily extensible.

In addition to enhancing security of a digital
transmission, dynamic encryption in accordance with the
present invention allows for only partial encryption of the
data stream, which is especially useful for video and audio
data since the stream can be rendered almost impossible to
comfortably view or listen to by encrypting relatively
small fractions of the overall data. Further, the ability
to partially encrypt a transmission allows a system to
control the amount of resources, for example, CPU cycles if
the encryption or decryption is performed by software, used
in the encryption or decryption of a data stream. And,
"overhead" of transmitting encryption parameters may be
controlled by updating the one or more parameters less
frequently if bandwidth is a concern. By providing an
encryption parameter set, different levels of
"thoroughness" can be achieved in encrypting the data. For
example, where a digital data transmission is of high
priority, a large percentage of the transmission may be
encrypted, and further, the encryption key (or other
encryption parameter) may be changed frequently with the
content of the data. If desired, encryption parameters may
be multiplexed (i.e., joined) with the actual payload data

when transmitted. In addition to helping to disguise the fact that the data is encrypted, no additional data paths for transmission of the encryption parameters would be required in such an implementation.

5 ## Brief Description of the Drawings

The above-described objects, advantages and features of the present invention, as well as others, will be more readily understood from the following detailed description of certain preferred embodiments of the invention, when
10 considered in conjunction with the accompanying drawings in which:

FIG. 1 depicts one embodiment of a system employing dynamic encryption and decryption in accordance with the
15 principles of the present invention; and

FIG. 2 is a flowchart of one embodiment for implementing dynamic encryption in accordance with the principles of the present invention by varying an encryption key from a set of established encryption
20 parameters.

Best Mode for Carrying Out the Invention

Generally stated, presented herein is a more secure method to encrypt a digital transmission by varying one or more encryption parameters over different portions the
25 stream of data. At certain data intervals, the encryption

scheme is changed, or more particularly, an encryption parameter such as an encryption key is modified. A next key in an evolving sequence of keys might be transmitted explicitly in the data stream by inserting it into the

5 stream or the key might be hidden in some unused bits in the stream. Alternatively, a predetermined transformation might be applied to the encryption parameter, for example, by incrementing it, or running the parameter through a hardware circuit.

10 A change in encryption method or encryption parameter may be signaled by an external signal, or the presence of something within the stream itself, or the occurrence of a pre-specified number of events. For example, an encryption key might be altered based on a certain number of bits or

15 bytes that have been transmitted and received, or based on a certain number of structures having been transmitted and received. Using an MPEG video data stream, this might mean that after a certain number of macroblocks, slices, fields, frames, pictures, groups of pictures (GOPs), or sequences

20 have been sent and received, an encryption parameter (such as an encryption key) is automatically updated. Many digital compression schemes allow for the inclusion of timing information (i.e., timestamps), often used for synchronization purposes.

25 Another scheme might be that sender and receiver change their encryption scheme, or update encryption keys, based upon timestamps passing certain prespecified threshholds, or upon passing certain threshholds as

designated by an external clock to which both sender and receiver have access. Recognition of signals indicating that the encryption scheme or key should be updated can be performed by dedicated hardware, or by software running on a host processor, as will be apparent to those skilled in the art.

In addition to dynamically encrypting a digital transmission, such as an MPEG video stream, encryption in accordance with the present invention can be partial or complete depending upon the importance of the data itself. For example, MPEG video consists of several "layers" of data, the largest of these might be an entire program, such as a movie, video-phone transmission, etc., and the smallest a macroblock of data. From the largest to the smallest, an MPEG stream can be described as including the following units: program, sequence, group of pictures (GOPs), picture, slice, and macroblock. Thus, in accordance with the principles of the present invention, the dynamic encrypting can occur at any one of these levels. Obviously, the amount of bandwidth required may vary with the level of encryption selected.

In addition, the MPEG standard allows for several optional types of "private" data, allows for many optional fields and extensions, and contains routine audio/video synchronization data known as "timestamps" (for example, presentation timestamps and decoding timestamps). Furthermore, MPEG streams are commonly divided and packaged into discrete packets known as "transport" packets, which

may be joined to create a transport stream. The transport stream architecture also allows for private data transmissions, and allows for optional fields and contains timestamp data as well. Any of these types of private data

5   could be employed in forwarding a dynamically modified encryption parameter from a sender to a receiver in a system employing the dynamic encrypting of the present invention.

Advantageously, dynamic encryption as presented herein

10   provides a more secure transmission of data, while still being flexible. For example, an MPEG stream may be transmitted using varying levels of encryption depending upon the sensitivity of the video material. A highly sensitive conference call, therefore, might be fully or

15   almost fully encrypted, while a public access program, or a non-confidential phone call might have a relatively low degree of encryption. Particularly where encryption and/or decryption involves software, the present invention allows the number of processor cycles needed for the encryption/

20   decryption to be controlled.

Note that a compressed audio stream (for example, MPEG audio, Dolby AC-3 audio, etc.) can be treated analogously to video as pertains to the use of the present invention. An audio stream might be said to consist of, from largest

25   to smallest units, a program, a frame, and a sample.

As one detailed example, dynamic encryption in accordance with the present invention may involve a set encryption parameters which includes:

Initial encryption key

5   This might be a key agreed upon in advance by the encryption and decryption units. Alternatively, the key might be randomly chosen then transmitted independently of the stream, or multiplexed into the stream, using private data packets or one or more fields of unused or reserved

10   bits according to the MPEG architecture. Further, some portion of the stream itself might serve as the initial key, with data beginning at, for example, some fixed offset of the payload, or the offset itself could be transmitted. The initial key, if transmitted more than once, may be

15   accompanied by "dummy" data designed to mislead an unauthorized observer attempting to decrypt the transmission. The initial key might itself be encrypted, and need to be decrypted before use.

Granularity

20   Granularity refers to the sub-units of MPEG data which are to be encrypted (also referred to herein as the "encryption units" or "units of encryption"). As mentioned above, a set of granularities for MPEG video data might be: program, sequence, group of pictures, picture, slice, and

25   macroblock. Once again, the granularity might be transmitted independently of the stream, or multiplexed into the stream, either as "private" data, or embedded in one or more unused MPEG fields.

Density scale

This is a number which will denote 100% encryption of
encryption units. For example, suppose the density scale
is 1024. Then a density (see below) of 1024 would indicate
5   100% encryption. A density of less than 1024 indicates
that not all encryption units are to be encrypted. The
density scale may be transmitted in any of the manners
described above, or simply agreed upon in advance.

Density

10   This refers to the fraction of the total units of
encryption which will be encrypted. This might be
communicated in terms of a predefined scale; for example,
the number 1024 might indicate 100% encryption. Then a
density of 512 would imply that every other encryption unit
15   is to be encrypted. Similarly, a density of 1 would
indicate that only one encryption unit out of each group of
1024 encryption units is to be encrypted. The density may
be transmitted in any of the manners described above.

Delay

20   This refers to the number of encryption units to wait
before encrypting the first one. This number is zero-
origin.

Key update unit

25   This refers to the unit which is to be tabulated in
order to determine when the encryption key is to be
updated. This unit might be one of the granularities
described above (picture, slice, etc.). For example, the

key is to be updated every n slices. Alternatively, the
key update unit might be bytes of data, for instance, the
key is to be updated every n bytes of transmission, or the
key update unit might be seconds (or milliseconds, etc.).

5   Key update data trigger
          This refers to the data interval at which the key is
to be refreshed. As noted above, The key might be newly
transmitted, independently of the stream, or multiplexed
into it. Alternatively, the existing key may be operated
10   on in some fashion, for example, to clock it through a
linear feedback shift register (LFSR), or to add a delta to
the existing key. Further, the key might be newly acquired
from the payload of the stream itself, at some
predetermined offset, or at some communicated offset. In
15   the case in which the key update unit is, for example, a
number of milliseconds, the stream's timestamps may be
examined, and the key updated at any picture whose
timestamp indicates that the key update interval has been
reached.

20   Any of the parameters described above may have default
values, in which case they do not need to be established
explicitly. The parameters may be communicated separately,
or combined into one number before transmission.
Dynamically encrypting in accordance with the present
25   invention can easily be extended to dynamically changing
encryption parameters other than the encryption key.

As one specific example, the following encryption parameters may be established:

>   granularity = slice
>   density sale = 1024
5   density = 256
>   delay = 1
>   key update unit = picture
>   key update frequency = 16

These parameters imply the following. The unit which
10   will be encrypted is the picture slice. One fourth of the
slices (256/1024) (i.e., every fourth slice) will be
encrypted. Further, the first slice will be unencrypted;
encryption will begin with the second slice (delay of 1)
and continue with every fourth slice thereafter. The
15   encryption key, after having been initialized, will be
updated at the start of every sixteenth picture (key update
frequency).

Refer now to FIG. 1, where one example of a system,
generally denoted 10, incorporating dynamic encryption in
20   accordance with the principles of the present invention is
depicted. System 10 includes a sender 12 and a receiver
14. Dynamically encrypted data is transmitted between
sender and receiver across any conventional transmission
medium 16. In this example, the data to be encrypted is
25   assumed to comprise a stream of MPEG data.

Sender 12 includes an encryption unit 20 which (in
this example) receives as inputs an encryption key from a
dynamic key generator 22, and the unencrypted, but encoded
MPEG data stream. Any conventional encryption technique
5   can be employed within encryption unit 20, provided that
the encryption can be modified dynamically as presented
herein by changing an encryption key or one or more other
encryption parameters as discussed above. Output from
encryption unit 20 is an encrypted MPEG stream. In this
10   example, the encrypted MPEG stream is fed to a data
multiplexer 24 which multiplexes into the stream the
encryption key employed to encrypt the stream and the
encryption parameters employed by the encryption unit.
Data multiplexer 24 is optional since the encryption key
15   and encryption parameters could be forwarded independent
from the encrypted stream of data, for example, on a
dedicated line (not shown) to the receiver 14.

Receiver 14 receives the dynamically encrypted stream
of data at a data demultiplexer 30, which again assumes
20   that the encryption key or encryption parameters have been
multiplexed into the stream. Output from demultiplexer 30
is the encryption key and/or parameters, as well as the
encrypted MPEG stream. This data is forwarded to a
decryption unit 32 which then decrypts the data using the
25   encryption information and provides an unencrypted MPEG
stream to a conventional MPEG decoder 34.

FIG. 2 is a flowchart of one embodiment of a dynamic
encryption routine in accordance with the principles of the

present invention. Processing begins by determining
appropriate encryption parameters based on sensitivity of
the transmitted data 100. As one example, the set of
encryption parameters may include encryption granularity,

5   density, delay, key update unit, and key update data
trigger, as the terms are defined herein. An initial
encryption key is established 110 and a first or next
portion of the MPEG data stream is encrypted 120 using the
encryption parameters and key. Assuming the existence of a

10   system such as depicted in FIG. 1, the key (and other
parameters if at the stream's beginning) is multiplexed
into the data stream 130 and transmitted 140 to a receiver.
Processing then determines whether the end of the stream
has been reached 150, and if so, dynamic encryption

15   processing is complete 160. Otherwise, processing
determines whether the encryption key needs to be updated
170. If yes, then the encryption key is updated 180 and
processing encrypts the next portion of the MPEG stream
120.

20   Note that, while decryption may be performed entirely
independently of and before MPEG decoding (as depicted in
FIG. 1), the decryption unit and MPEG decoder may be
integrated as a single unit. Such a discrete unit could be
designed to function properly for "normal" (i.e.,

25   unencrypted) MPEG streams, but to recognize encrypted
streams and to decrypt them before decoding is performed.

Note also, that in the case in which a key varies
according to content of the transmission, or according to

events in a transmission, a data error or loss can have
consequences since not only is a portion of the compressed
MPEG data potentially in error, but the decryption
mechanism may now be out of synchronization with the
5   transmitter's encrypter. One mechanism for dealing with
such a problem is to return to using the initial key at a
certain predefined interval (similar to the MPEG notion of
sequence headers). For example, at every sequence header,
or every GOP, the encrypter and decrypter both return to
10   using the initial key, which evolves from there. This
means that a data loss or error would be limited to
affecting only that sequence or group, after which
synchronization would be resumed. This would also
facilitate random access; that is, jumping from one place
15   in an MPEG stream to another.

Another mechanism, in a scenario in which keys are
delivered in the stream itself, is to simply deliver the
keys redundantly, that is, more often than they are needed
or updated.

20   A mechanism for determining that encryption/decryption
synchronization has been lost might be to place a signal in
the first unit of encryption (whether encrypted or not)
after a key change. If the decrypter sees such a signal,
and has not updated its key since the last such signal,
25   then the decrypter knows that synchronization has been
lost. Likewise, if the decrypter updates its key and fails
to see such a signal in the next unit of encryption, it

also knows that synchronization has been lost, and can take appropriate action (for example, notify the transmitter, or wait for the next point at which the encryption key can be reliably re-established). This would only require the use

5   of a single spare bit in an encryption unit.

When transmitting "elementary" MPEG video data, parameters may, for example, be stored in any combination of the following structures:

- One or more "user_data" field(s).
10   The "copyright_extension" construct, specifically by setting the "copyright_flag" to 0 and using fields "copyright_number_1", "copyright_number_2", and "copyright_number_3".
- The "time_code" field in a "group of pictures header"
15   (this field is not used during decoding).

When transmitting MPEG in "program stream" form, parameter data may be conveyed by any of the methods above, or further, in "PES" packets (PES denoting "packetized elementary system") of a specific type. The content type

20   of PES packets is defined by the PES packet's "stream_id" field. The MPEG 2 specification defines a "stream_id" value denoting a "private_stream_1" packet, and another denoting a "private_stream_2" packet. These types are slightly different, but can contain anything the user

25   wishes. Of course, the more overtly parameters and keys are transmitted, the less overall security.

When transmitting MPEG data in "transport stream"
format, parameter data may be conveyed by any of the above
methods, or further, such data may be stored as
"private_data bytes" in the "adaption_field" structure.

5   To restate, provided herein is a secure technique for
encrypting a digital data stream by dynamically varying one
or more encryption parameters employed in encrypting the
data. Varying of the encryption parameter(s) is preferably
responsive to data content. For example, one trigger might
10   be the passage of a certain number of units, where units
are specific to the format in which the data is stored.
For a digital stream, units would typically be bits, bytes,
words, blocks, etc. (and in the distant future, such units,
in a biological computer, would be cells, tissue, organs,
15   organism). Alternatively, the trigger for changing the
encryption parameter could be the passage of a certain
number of units, where the units are specific to the
content of the data. In an MPEG stream, the data
represents a program composed of sequences, groups of
20   pictures, pictures, slices, macroblocks. In the case of a
book, for example, the data could be said to represent a
volume, title(s) within the volume, pages, paragraphs,
sentences, words, letters. Thus, a first trigger could
depend on the passage of units of physical data, and these
25   physical units would be the same no matter the type of
information represented. A second trigger could depend on
the passage of conceptual units of data, and these units
would generally be specific to the content of the data.

The present invention can be included, for example, in an article of manufacture (e.g., one or more computer program products) having, for instance, computer usable media. This media has embodied therein, for instance,

5   computer readable program code means for providing and facilitating the capabilities of the present invention. The articles of manufacture can be included as part of the computer system or sold separately.

Additionally, at least one program storage device

10   readable by machine, tangibly embodying at least one program of instructions executable by the machine, to perform the capabilities of the present invention, can be provided.

The flow diagrams depicted herein are provided by way

15   of example. There may be variations to these diagrams or the steps (or operations) described herein without departing from the spirit of the invention. For instance, in certain cases, the steps may be performed in differing order, or steps may be added, deleted or modified. All of

20   these variations are considered to comprise part of the present invention as recited in the appended claims.

While the invention has been described in detail herein in accordance with certain preferred embodiments thereof, many modifications and changes therein may be

effected by those skilled in the art. Accordingly, it is intended by the appended claims to cover all such modifications and changes as fall within the true spirit and scope of the invention.

Claims

1   1.   A method for protecting a stream of data to be
2   transferred between an encryption unit and a
3   decryption unit, said method comprising:

4   encrypting the stream of data at said encryption
5   unit for transferring of said encrypted stream of data
6   from said encryption unit to said decryption unit;

7   dynamically varying said encrypting of said
8   stream of data at said encryption unit by changing at
9   least one encryption parameter and signaling said
10   change in encryption parameter to said decryption
11   unit, said dynamically varying of said at least one
12   encryption parameter being responsive to occurrence of
13   a predefined condition in said stream of data; and

14   decrypting said encrypted data at the decryption
15   unit, said decrypting accounting for said dynamic
16   varying of said encrypting by said encryption unit
17   using said changed encryption parameter.

1   2.   The method of claim 1, wherein said at least one
2   encryption parameter comprises at least one of an
3   encryption key, an encryption granularity, an encryption
4   density scale, an encryption density, an encryption delay,
5   an encryption key update variable, and an encryption key
6   update data trigger.

1   3.   The method of claim 2, wherein said at least one
2   encryption parameter comprises at least some of said
3   encryption key, encryption granularity, encryption density
4   scale, encryption density, encryption delay, encryption key
5   update variable, and encryption key update data trigger.

1   4.   The method of claim 2, further comprising
2   multiplexing said changed encryption parameter and said
3   encrypted data at a sender prior to transferring thereof to
4   a receiver containing said decryption unit, and
5   demultiplexing said changed encryption parameter and said
6   encrypted data at said receiver.

1   5.   The method of claim 1, wherein said dynamically
2   varying comprises dynamically varying said encryption
3   parameter based on passage of a predefined number of units
4   of physical data or passage of a predefined number of
5   conceptual units of data.

1   6.   The method of claim 5, wherein said encryption
2   parameter comprises an encryption key.

1   7.   The method of claim 1, wherein said stream of
2   data comprises a stream of compressed data, and wherein
3   said method further comprises decompressing said compressed
4   data after said decrypting of said encrypted data by said
5   decryption unit.

1   8.   The method of claim 7, wherein said stream of
2   compressed data can comprise one of MPEG encoded video
3   data, MPEG encoded audio data, and Dolby AC-3 audio data.

1   9.   The method of claim 1, further comprising
2   initializing a plurality of encryption parameters based on
3   sensitivity of said stream of data, said plurality of
4   encryption parameters being employed by said encrypting and
5   wherein said changed encryption parameter of said
6   dynamically varying comprises one encryption parameter of
7   said plurality of encryption parameters.

1   10.   The method of claim 1, wherein said stream of
2   data comprises a stream of MPEG compressed data, and said
3   method further comprises setting a plurality of encryption
4   parameters for use by said encrypting based upon
5   sensitivity of said stream of MPEG compressed data, and
6   wherein said changed encryption parameter comprises one
7   encryption parameter of said plurality of encryption
8   parameters.

1   11.   The method of claim 10, wherein said setting of
2   said plurality of encryption parameters includes
3   establishing at least some of an encryption granularity, an
4   initial encryption key, a density scale, a density, an
5   encryption delay, and a key update data trigger for said
6   stream of MPEG encoded data.

1   12. The method of claim 1, wherein said encrypting

2 comprises encrypting multiple portions of said data stream,

3 and wherein said dynamically varying comprises dynamically

4 varying said encrypting of said multiple portions of said

5 data stream by changing said at least one encryption

6 parameter for each portion of said multiple portions.

1   13. The method of claim 1, wherein said dynamically

2 varying comprises dynamically varying said at least one

3 encryption parameter responsive to passage of a predefined

4 number of data bits in said stream of data, or

5 alternatively, responsive to passage of a predefined number

6 of data units in said stream of data, wherein said data

7 units comprise at least one of a program, a sequence, a

8 group of pictures, a picture, a slice, or a macroblock.

1   14. A system for protecting a stream of data

2 comprising:

3   an encryption unit for encrypting the stream of

4 data for transfer to a decryption unit;

5   means for dynamically varying said encrypting of

6 said stream of data by said encryption unit by changing an

7 encryption parameter and signaling said change in

8 encryption parameter to said decryption unit, said means

9 for dynamically varying being responsive to occurrence of a

10 predefined condition in said stream of data; and

11   wherein said decryption unit decrypts said
12   encrypted data, said decrypting accounting for said
13   dynamic varying of said encrypting by said encryption
14   unit using said changed encryption parameter.

1   15. The system of claim 14, wherein said changed
2   encryption parameter comprises an encryption key, and
3   wherein said means for dynamically varying comprises a
4   dynamic encryption key generator, and means for dynamically
5   varying said encryption key based on an occurrence of a
6   predefined condition in said stream of data.

1   16. The system of claim 15, wherein said stream of
2   data comprises a stream of digital data.

1   17. The system of claim 14, wherein said means for
2   dynamically varying comprises means for dynamically varying
3   said encryption parameter based on passage of a predefined
4   number of units of physical data or passage of a predefined
5   number of conceptual units of data.

1   18. The system of claim 14, wherein said encryption
2   unit encrypts multiple portions of the stream of data, and
3   wherein said means for dynamically varying comprises means
4   for changing said encryption parameter for each portion of
5   said multiple portions of said stream of data.

1   19. The system of claim 14, wherein said at least one
2   encryption parameter comprises at least one of an
3   encryption key, an encryption granularity, an encryption
4   density scale, an encryption density, an encryption delay,
5   an encryption key update variable, and an encryption key
6   update data trigger.

1   20. The system of claim 19, wherein said at least one
2   encryption parameter comprises at least some of said
3   encryption key, encryption granularity, encryption density
4   scale, encryption density, encryption delay, encryption key
5   update variable, and encryption key update data trigger.

1   21. The system of claim 14, further comprising a data
2   multiplexer for multiplexing said changed encryption
3   parameter into said encrypted data for transfer thereof to
4   said decryption unit.

1   22. The system of claim 14, further comprising means
2   for setting a plurality of encryption parameters based on
3   sensitivity of said stream of data, said plurality of
4   encryption parameters being employed by said encryption
5   unit and wherein said changed encryption parameter
6   comprises one encryption parameter of said plurality of
7   encryption parameters.

1   23. The system of claim 22, wherein said stream of
2   data comprises a stream of compressed data, and wherein
3   said system further comprises a decoder for decompressing
4   said compressed data after decrypting thereof by said
5   decryption unit.

1   24. The system of claim 23, wherein said stream of
2   compressed data can comprise a stream of one of MPEG
3   encoded video data, MPEG encoded audio data, and Dolby AC-3
4   audio data.

1   25. The system of claim 22, wherein said means for
2   setting said plurality of encryption parameters includes
3   means for establishing at least some of an encryption
4   granularity, an encryption key, a density scale, a density,
5   an encryption delay, and a key update data trigger.

1   26. The system of claim 14, wherein said means for
2   dynamically varying comprises means for changing said
3   encryption parameter based on a predefined number of bits
4   being encoded by said encryption unit, or alternatively,
5   based on a predefined number of units being encoded by said
6   encryption unit, said units comprising one of a program, a
7   sequence, a group of pictures, a picture, a slice, or a
8   macroblock.

1   27. A system for protecting a stream of data to be
2   transferred between a sender and a receiver, said system
3   comprising:

4   an encryption unit disposed at said sender for

5   encrypting the stream of data prior to transfer to

6 said receiver, said encryption unit being adapted to

7 dynamically vary encrypting of the stream of data by

8 changing at least one encryption parameter based on an

9   occurrence of a predefined condition in said data

10   stream and signaling said change in encryption

11   parameter to said receiver; and

12   a decryption unit disposed at said receiver for

13   decrypting said encrypted data, said decryption unit

14   being adapted to receive said changed encryption

15   parameter to account for said dynamic varying of said

16   encrypting by said encryption unit using said changed

17   encryption parameter.

1   28. At least one program storage device readable by a

2 machine, tangibly embodying at least one program of

3 instructions executable by the machine to perform a method

4 for protecting a stream of data to be transferred between

5 an encryption unit and a decryption unit, comprising;

6   encrypting the stream of data at said

7   encryption unit for transfer thereof to said

8   decryption unit;

9   dynamically varying said encrypting of said

10   stream of data at said encryption unit by changing an

11   encryption parameter and signaling said change in

12   encryption parameter to said decryption unit, wherein

13   said dynamically varying of said encryption parameter

14   is responsive to occurrence of a predefined condition

15   in said stream of data; and

16   decrypting said encrypted data at the

17   decryption unit, said decrypting accounting for said

18   dynamic varying of said encrypting by said encryption

19   unit using said changed encryption parameter.

1   29. The at least one program storage device of claim

2   28, wherein said encryption parameter comprises at least

3   one of an encryption key, an encryption granularity, an

4   encryption density scale, an encryption density, an

5   encryption delay, an encryption key update variable, and an

6   encryption key update data trigger.

1   30. The at least one program storage device of claim

2   29, wherein said at least one encryption parameter

3   comprises at least some of said encryption key, encryption

4   granularity, encryption density scale, encryption density,

5   encryption delay, encryption key update variable, and

6   encryption key update data trigger.

1   31. The at least one program storage device of claim

2   29, wherein said method further comprises multiplexing said

3   changed encryption parameter and said encrypted data at a

4   sender prior to transferring thereof to a receiver

5   containing said decryption unit, and demultiplexing said

6   changed encryption parameter and said encrypted data at

7   said receiver.

1   32. The at least one program storage device of claim
2   28, wherein said dynamically varying comprises dynamically
3   varying said encryption parameter based on passage of a
4   predefined number of units of physical data or passage of a
5   predefined number of conceptual units of data.

1   33. The at least one program storage device of claim
2   32, wherein said encryption parameter comprises an
3   encryption key.

1   34. The at least one program storage device of claim
2   28, wherein said stream of data comprises a stream of
3   compressed data, and wherein said method further comprises
4   decompressing said compressed data after said decrypting of
5   said encrypted data by said decryption unit.

1   35. The at least one program storage device of claim
2   34, wherein said stream of compressed data can comprise one
3   of MPEG encoded video data, MPEG encoded audio data, and
4   Dolby AC-3 audio data.

1   36. The at least one program storage device of claim
2   28, wherein said method further comprises initializing a
3   plurality of encryption parameters based on sensitivity of
4   said stream of data, said plurality of encryption
5   parameters being employed by said encrypting and wherein
6   said changed encryption parameter of said dynamically
7   varying comprises one encryption parameter of said

8   plurality of encryption parameters.

1   37. The at least one program storage device of claim
2   28, wherein said stream of data comprises a stream of MPEG
3   compressed data, and said method further comprises setting
4   a plurality of encryption parameters for use by said
5   encrypting based upon sensitivity of said stream of MPEG
6   compressed data, and wherein said changed encryption
7   parameter comprises one encryption parameter of said
8   plurality of encryption parameters.

1   38. The at least one program storage device of claim
2   37, wherein said setting of said plurality of encryption
3   parameters includes establishing at least some of an
4   encryption granularity, an initial encryption key, a
5   density scale, a density, an encryption delay, and a key
6   update data trigger for said stream of MPEG encoded data.

DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA

Abstract of the Disclosure

Dynamic varying of encrypting of a stream of data at an encryption unit based on data content is disclosed. The dynamic varying of the encrypting, which can be responsive to passage of a predefined number of units of physical data or passage of a predefined number of conceptual units of data, is accomplished by changing at least one encryption parameter over different portions of the data. The at least one encryption parameter can comprise one or more of an encryption key, an encryption granularity, an encryption density scale, an encryption density, an encryption delay, an encryption key update variable, and an encryption key update data trigger. The change in encryption parameter is signaled to a receiver's decryption unit and used by the decryption unit in decrypting the dynamically varied encrypted stream of data. The stream of data may comprise, e.g., MPEG compressed video or audio.
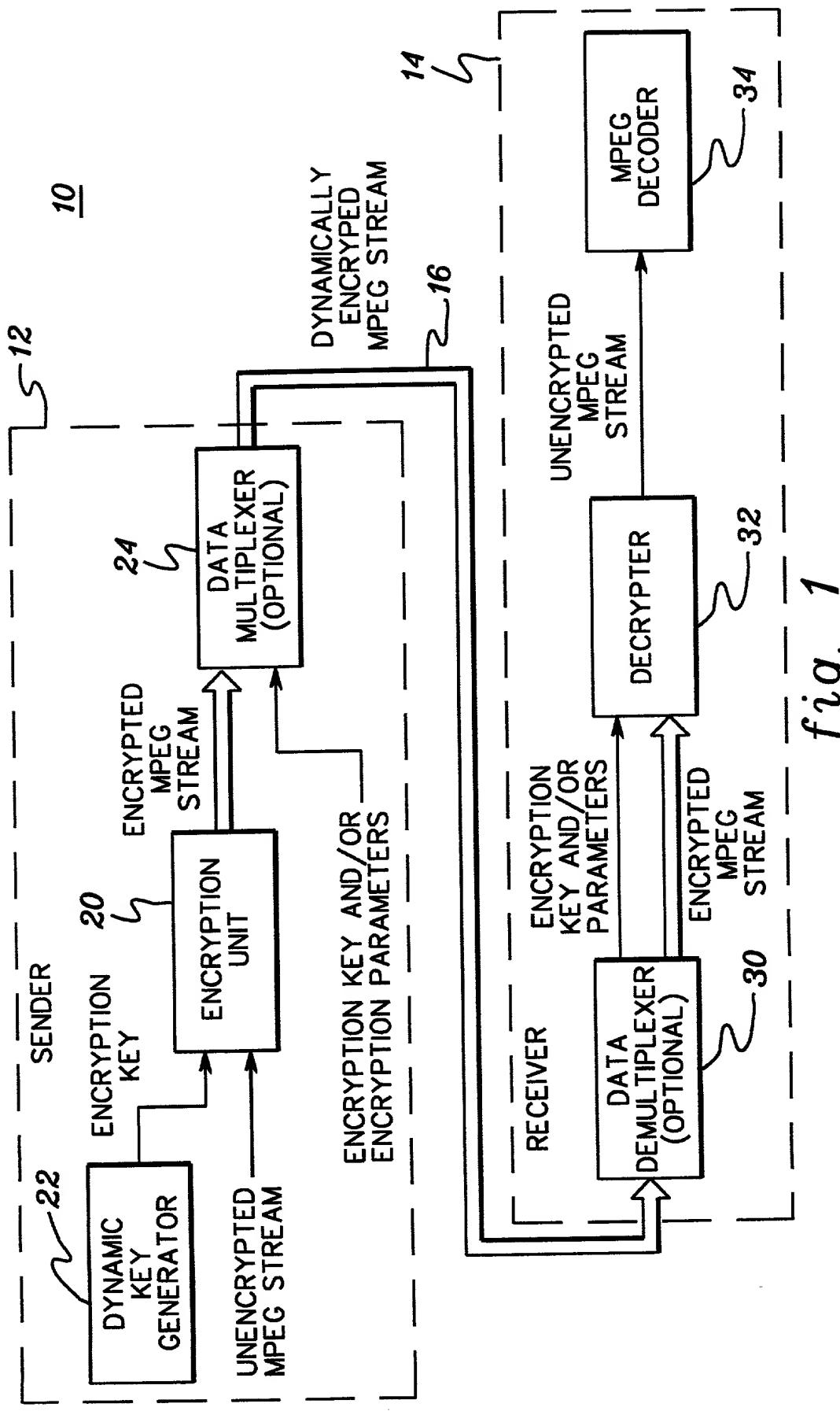
EN998146   33

fig. 1
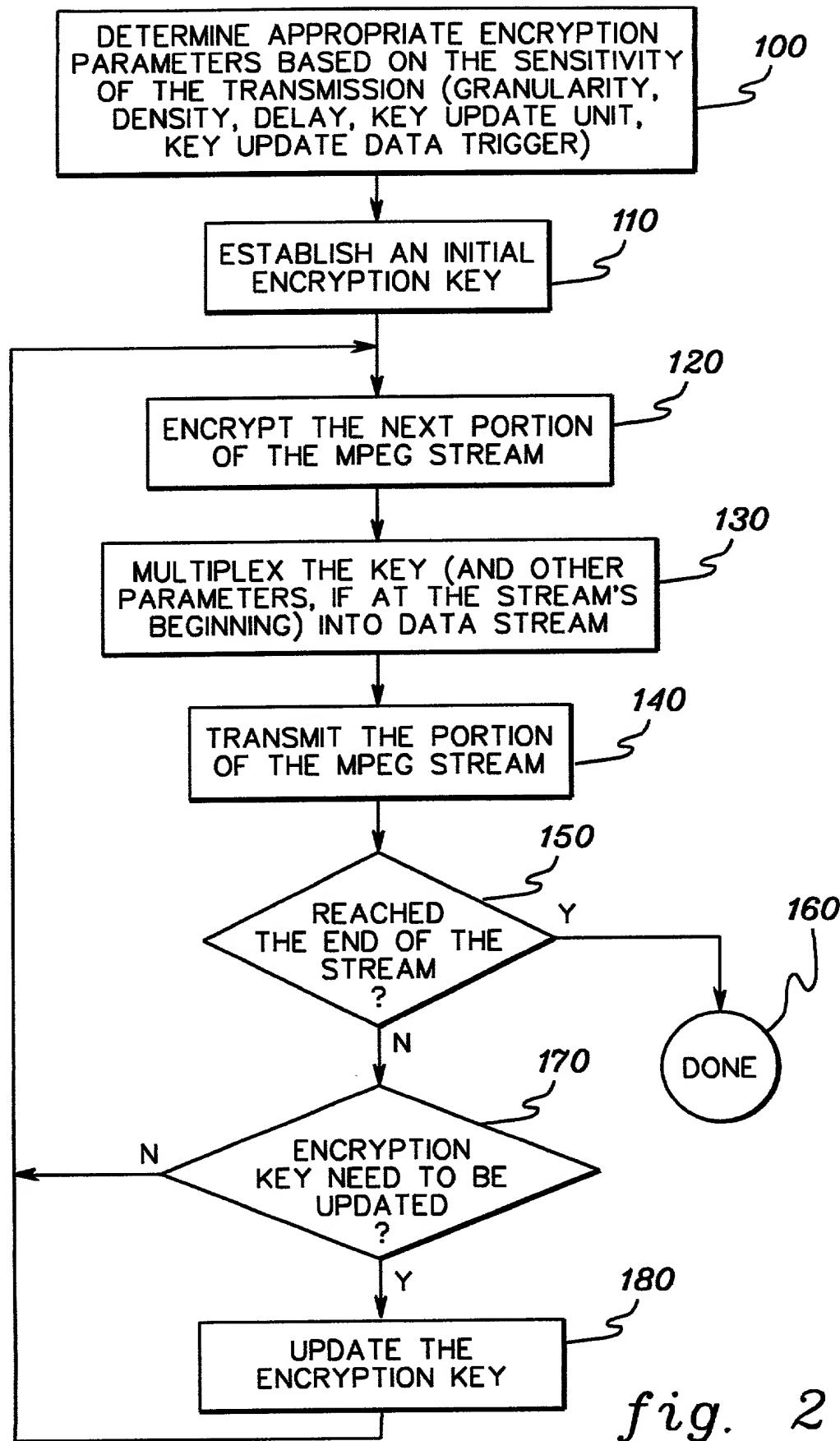
*fig. 2*

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International

Application Number _____

and was amended on _____

<div align="center">(if applicable)</div>

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Not Claimed

			☐
(Number)	(Country)	(Day/Month/Year Filed)	
			☐
(Number)	(Country)	(Day/Month/Year Filed)	
			☐
(Number)	(Country)	(Day/Month/Year Filed)	

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional

(Application Serial No.)	(Filing Date)

(Application Serial No.)	(Filing Date)

(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Christopher A. Hughes, Esq., Reg. No. 26,914   Blanche E. Schiller, Esq., Reg. No. 35,670
Edward A. Pennington, Esq., Reg. No. 32,588
John E. Hoel, Esq., Reg. No. 26,279
Joseph C. Redmond, Jr., Esq., Reg. No. 18,753
David L. Adour, Esq., Reg. No. 29,604
Lawrence R. Fraley, Esq., Reg. No. 26,885
Arthur J. Samodovitz, Esq., Reg. No. 31,297
William H. Steinberg, Esq., Reg. No. 28,540
John R. Pivnichny, Ph.D., Reg. No. 43,001
Jeff Rothenberg, Esq., Reg. No. 26,429
Kevin P. Radigan, Esq., Reg. No. 31,789

Send Correspondence to: **Kevin P. Radigan, Esq.**
HESLIN & ROTHENBERG, P.C.
5 Columbia Circle
Albany, N.Y. 12203-5160

Direct Telephone Calls to: *(name and telephone number)*
Kevin P. Radigan, Esq. (518) 452-5600

Full name of sole or first inventor **John Edward Fetkovich**	
Sole or first inventor's signature	Date *October 13, 1999*
Residence **427 River Terrace, Apt. F-3, Endicott, N.Y. 13760**	
Citizenship **United States of America**	
Post Office Address **427 River Terrace, Apt. F-3, Endicott, N.Y. 13760**	

Full name of second inventor, if any **Wai Man Lam**	
Second inventor's signature	Date *Nov 15, 99*
Residence **1325 Sunny Ridge Road, Moheganlake, N.Y. 10547**	
Citizenship **Hong Kong**	
Post Office Address **1325 Sunny Ridge Road, Moheganlake, N.Y. 10547**	

Full name of third inventor, if any
George William Wilhelm, Jr.

Third inventor's signature _George William Wilhelm Jr._

Date **10/14/99**

Residence
705 Catalina Boulevard, Endwell, N.Y. 13760-1611

Citizenship
United States of America

Post Office Address
705 Catalina Boulevard, Endwell, N.Y. 13760-1611

Full name of fourth inventor, if any

Fourth inventor's signature

Date

Residence

Citizenship

Post Office Address

Full name of fifth inventor, if any

Fifth inventor's signature

Date

Residence

Citizenship

Post Office Address

Full name of sixth inventor, if any

Sixth inventor's signature

Date

Residence

Citizenship

Post Office Address